# Proposal for Wisconsin Collaboration on Secure Messaging Gateways for Internet E-mail

## Why do we need secure Internet E-mail?

An increasing amount of public and private business relies on E-mail for rapid, documented, efficient communication. Some E-mails contain sensitive information, including protected health information (PHI). E-mail sent over the Internet has a small but real probability of being improperly observed, especially at relay points. While neither the HIPAA privacy nor security rule expressly requires it, most people involved with HIPAA believe secure internet E-mail is necessary for a covered entity's due diligence in abiding by the HIPAA *law's* requirement to "ensure the integrity and confidentiality" of PHI.

## What are the business requirements for secure Internet E-mail?

### Encryption

Secure E-mail basically means E-mail that is encrypted at a sufficiently robust level, usually at least 128-bits. Most E-mail systems can encrypt E-mails in transit and at rest within the given system. For example, at the Wisconsin Department of Health and Family Services (DHFS), E-mails within the GroupWise system are encrypted in transit anywhere on our wide area network (WAN) and stored in an encrypted form managed by GroupWise.

### B2B Focus

The focus of this paper is on organizations, rather than individuals. The primary business use of Internet E-mail today is between organizations and thus the most pressing need is for a business-to-business (B2B) solution. Business-to-consumer (or client) (B2C) use of E-mail is growing but currently less common. There is also greater immediate pressure for secure B2B E-mail because B2C privacy concerns can be at least temporarily addressed by obtaining client authorization for the use of E-mail. The requirements and preferred solutions for these two kinds of use vary. Any solution for secure Internet E-mail should first meet the B2B requirements but also not be inconsistent with supporting B2C needs.

### E-mail System Integration

Most organizations have a legacy commitment to their E-mail systems and the messages within them. E-mail systems are not going away anytime soon. The secure Internet E-mail solution should recognize this commitment and work seamlessly with these existing systems.

### Simplicity of Use

The E-mail system integration requirement dovetails with another: use of secure Internet E-mail should be transparent to the user. The effective interoperability of most E-mail systems today has accustomed users to a high ease-of-use standard. Sending, receiving,

reading, and storing secure Internet E-mail should be done through the organization's current E-mail system with minimal complexity and training for the user and little need for desktop support.

**Enforcement**
The secure Internet E-mail solution should help ensure that E-mails that should be secure actually are. Rather than rely solely on the user at the desktop to always remember and to make correct decisions about selecting the secure option for individual E-mails, some products can manage encryption based on who the recipient or sender is or other business rules.

**Continued Protection from E-mail-borne Threats**
It is nearly impossible to conduct virus checking or content filtering on encrypted E-mails. Some secure E-mail solutions interfere with these key activities.

**Record Management**
Most E-mail systems store E-mails on the user's desktop and/or organization's servers. The organization thus controls the retention and disposition of these important records. Not all secure Internet E-mail solutions support this control. Some vendor solutions store sent E-mails on their servers, and sometimes recipients have no control over received E-mails. Also, some solutions encrypt in such a way that organizations can not access stored E-mails of current or previous employees.

**Collaboration**
Among HIPAA security and privacy requirements, secure Internet E-mail is especially challenging because an organization can not implement it alone. Secure Internet E-mail by its nature requires collaboration between sending and receiving parties. And every organization has multiple such parties. Solving secure Internet E-mail requires collaboration among business partners. Regional voluntary organizations formed to help covered entities comply with HIPAA, like the HIPAA Collaborative of Wisconsin (COW), are well situated to promote such collaboration.

**Choice**
One outcome of collaboration could be agreement for all members to use the same product. This would be one approach to solving a continuing problem of limited interoperability of vendor secure Internet E-mail solutions. A better approach is to encourage purchaser choice via competition among multiple vendors with interoperability based on standards. Whether through the HIPAA security rule or otherwise, the federal government does not appear to be establishing a standard. Voluntary standards through vendor and purchaser collaboration will hopefully provide the needed interoperability.

**Future Requirements**
The immediate requirement of secure Internet E-mail for HIPAA compliance is encryption to avoid impermissible disclosure of PHI. Some vendor solutions for secure Internet E-mail provide capabilities for other requirements to which organizations will need to attend in the future. One is authentication of sender and receiver of secure

Internet E-mail. Related functions are digital signatures, proof of receipt and nonrepudiation (eliminating the ability to deny the identified party sent a valid message).

## Is there a solid technology foundation for secure Internet E-mail?

Public key cryptography is a well-established technology that uses private and public "keys" to encrypt and decrypt information. For example, if X wants to send Y an encrypted E-mail, X first obtains Y's public key. X encrypts his message with this public key and sends the encrypted E-mail to Y. Y decrypts the E-mail using his own private key. X needs to obtain a public key from everyone to whom he wants to send an encrypted E-mail. Y has to do the same. After awhile, these keys expire. There has to be a source for valid keys. This technology is sometimes called PKI for Public Key Infrastructure—all the technology and administration involved in distributing and managing valid public keys.

This technology works well and is supported by most major E-mail systems today (with some vendor interoperability issues). It also addresses the identification, digital signature and non-repudiation requirements. Most observers believe PKI will be the long-term solution for secure Internet E-mail. Multipurpose Internet Mail Extensions (MIME) is the standard that allows interoperability between E-mail systems. S/MIME (Secure MIME) is a standard on top of MIME that allows interoperability for secure E-mail using PKI technology. The State of Wisconsin has adopted S/MIME as a draft standard for secure E-mail.

The main reason S/MIME and PKI have not been widely adopted is the complexity of administering the keys. As implemented in E-mail systems, keys are managed by the individual users at their desktops. Most users find the process confusing. Managing revoked and expiring certificates (which contain the keys and support the "trust model" needed to ensure that a public key belongs to whom it says it does) is a significant task for individuals and organizations.

## What approaches are there to secure Internet E-Mail?

There are four principal approaches to securing Internet E-mails.

### End-to-end (desktop) encryption

This approach uses S/MIME or other standards such as Pretty Good Privacy (PGP). Each individual user has a digital certificate/key. The E-mail remains encrypted until it reaches the desktop. This can work well technically but has several disadvantages.

- Managing the keys is burdensome
- Keys are no more secure than the desktops through which they are administered
- Because users can store E-mails encrypted with their personal key, management can lose control over these records, finding it extremely difficult if not impossible to decrypt messages deleted by employees or to access E-mails of separated employees
- It is nearly impossible to conduct virus or content filtering on encrypted messages

DHFS is currently piloting S/MIME desktop encryption with a few Medicaid HMOs. We are using our GroupWise 6 desktop clients to encrypt and decrypt. A few additional HMOs that wanted to pilot could not because their E-mail system versions were too old or did not support S/MIME at all. Because the number of users is small in each organization and few organizations are involved, the key management burden on users has been acceptable. Once keys are exchanged, sending and receiving secure E-mails is little different from those that are unencrypted.

Other communities, including the Commonwealth of Massachusetts and the New Zealand government, have attempted pilots of desktop S/MIME and have abandoned intentions to use the technology for broad-based deployment.

**Gateway-to-gateway (domain or server level) encryption**

This approach uses similar technology to desktop encryption but performs the encryption and decryption at a server rather than desktop client. Rather than assign each user a digital certificate/key, the keys are assigned at an organizational level. This has several differences from the desktop approach.

- There are radically fewer keys to manage
- Users are not burdened with key management
- Messages are encrypted over the Internet between organizations, but can be decrypted within the organization
- E-mails are stored on the servers of sending and receiving organizations and remain under their control
- Management retains control over its records
- Virus checking and content filtering are possible
- Applications can use gateways to send or receive messages
- "Trust" is established at the organizational rather than individual level.

This approach can work seamlessly with legacy E-mail systems—the user sends, receives, manages E-mails within their E-mail client. Administration is simpler, user burden reduced, and organizational control over E-mails retained. A major potential drawback is that identification occurs at the organization level rather than specific to individuals. For most business purposes, however, establishing "trust" at the organizational level should be sufficient. With this approach, business partners trust each other to manage their internal affairs such that specific users within each organization are reliably identified with means other than unique digital certificates (e.g., E-mail addresses).

New Zealand's SEE Mail initiative is a deployed gateway encryption environment, and Massachusetts has completed a pilot program that demonstrated the potential of this approach.

**Secure WEB Mail**

In this approach, the sender posts a sensitive message to a secure web site using an encrypted transmission[i] . An unencrypted E-mail that points to an obscure URL is then sent to the recipient. The recipient accesses the sensitive message at the URL using a

secured session. The recipient uses an ID and password to access the secure session. The password is provided through a separate contact such as a telephone call or through self-registration by the recipient. This approach has the following advantages and disadvantages.

- The recipient only needs a web browser and Internet access.
- Users and organizations do not need to manage keys (beyond those used for session security)
- Messages can not be sent, read or managed through existing E-mail systems
- The message resides on the provider's server and
  - can be removed at any time by the sender
  - in many systems can not be downloaded, stored or managed by the recipient except by cutting and pasting the text or saving the HTML page
- Users must manage IDs and passwords for each partner with whom they conduct E-mail this way
- Strong user identification, non-repudiation and proof of receipt may be less rigorously supported
- Cannot perform virus scanning and content security checks due to use of SSL sessions for viewing and downloading.

This approach has the noted disadvantages compared to approaches that preserve an integration with existing E-mail systems. On the other hand, its main advantage is that such systems are not needed. This approach is the best alternative for business-to-client (B2C) secure Internet E-mail. Some of its disadvantages are lessened where many of the recipients (such as patients) will conduct secure Internet E-mail with only a few partners (such as doctors). It also works reasonably where one party (eg a doctor) conducts secure Internet E-mail with many others (eg patients). Where this works less well is where many parties conduct secure Internet E-mail with many other parties.

**HTML Attachment Approach**

In this approach, the message and any attachments to be secured are encrypted and placed in an HTML attachment to an unsecured E-mail. Java code in the attachment requires authentication of the recipient before it allows the attachment to be opened, decrypted and the secured information read. The unsecured message is received by the recipient through his or her usual E-mail system and can be stored and later managed by the recipient in his or her Inbox. To access the secure information the recipient opens the attachment, which launches his or her browser and activates the Java code. This approach has several significant advantages and a couple serious disadvantages.

- The recipient needs no additional software beyond a browser
- The recipient uses his or her existing E-mail system to receive, open and manage received messages
- The recipient does not need a commercial E-mail system, but can use web services such as Hotmail (so this solution also works relatively well for B2C)
- Proof of receipt can be supported in certain vendor products
- Through the Java code, senders can control the message after delivery, restricting access to the sender only or removing access after a predetermined period of time
- Because of the above sender controls, the recipient and his or her organization can lose control over the received message

- Virus checking and content security checks cannot be performed on these encrypted attachments.

## What is the Secure Messaging Gateways (SMG) Initiative?

The most pressing need, at least for health care organizations, is for a current capacity for secure Internet E-mail between organizations (B2B). If possible, the current solution should be consistent with the longer-term answer and provide a ready migration course to it. The long term secure E-mail answer appears to be based on digital certificates and the S/MIME standard, and will eventually offer individual authentication whether it is desktop based or not. For now, the best approach for inter-organization secure Internet E-mail seems to be the gateway-to-gateway option. The Gartner Group recognizes that "the market is moving toward a preference for server-side approaches"[ii]. Giga "recommends S/MIME solutions with an option of Web-based or HTML-attachment delivery".[iii] (Both advisory firms believe desktop S/MIME will be the long term standard).

A specific type of gateway-to-gateway secure Internet E-mail holds special promise: Secure Messaging Gateways (SMG). SMG is an emerging protocol for server-to-server encryption using S/MIME. S/MIME provides the protocol and format for such encryption, but SMG provides additional conventions for organization-level certificates instead of individual certificates.

At the March 2001 HealthKey Summit in Chicago, five vendors demonstrated the interoperability of their Secure Messaging Gateways. The Massachusetts Health Data Consortium (MHDC) is currently finalizing the SMG protocol and is piloting its production use in Massachusetts, where interoperability remains somewhat an issue.

The Open Group (www.opengroup.org) is a voluntary organization that promotes open standards and operates a product certification service for protocols such as UNIX and LDAP. The MHDC is currently collaborating with the Open Group to establish a product certification program for the SMG protocol. Their targets are to finish the SMG protocol by end of this year, and to begin certifying products between February and May of 2004. The Commonwealth of Massachusetts and members of the MHDC are ready to purchase these products once they are identified. Several vendors are currently involved in this effort.[iv]

## How can we get to secure Internet E-mail in Wisconsin?

As noted earlier, secure Internet E-mail is not a challenge individual organizations can solve themselves. Instead, cooperation between E-mailing business partners is necessary. Collaboration is needed between and among using organizations and vendors. Such collaboration can lead to consumer choice between competing vendor products, with interoperability assured by certification based on standards. The foundation for this approach exists in the SMG certification effort of the Massachusetts Health Data Consortium and the Open Group.

The HIPAA Coordinator for the Wisconsin Department of Health and Family Services (DHFS) wrote this paper. Our principal interest is to be able, as soon as practical, to interchange secure Internet E-mail (often containing protected health information) with our major business partners:

- county and municipal agencies
- HMOs
- health care and social service providers
- other payers including Medicare.

(Our limited but growing need to securely transmit E-mails to participants in our programs and members of the general public is currently a lesser concern.) Like the MHDC members, DHFS is looking to procure a product to secure Internet E-mail once a valid direction is established.

**A Wisconsin forum for collaboration**

The Workgroup for Electronic Data Exchange (WEDI) was a principal behind the creation of HIPAA. WEDI encourages regional collaboration among entities covered by HIPAA, through the Strategic National Implementation Program (SNIP). The non-profit HIPAA Collaborative of Wisconsin (COW) is a WEDI SNIP affiliate serving private and public parties impacted by HIPAA. HIPAA COW is an ideal forum to establish a consistent approach to secure Internet E-mail in Wisconsin, based on the health care core that must address secure Internet E-mail for HIPAA compliance. An endorsement of the SMG approach by HIPAA COW and voluntary commitment by its participating organizations to acquiring products from SMG certified vendors can provide the necessary foundation for an interoperable solution in Wisconsin. Once organizations acquire certified products, their interoperation can be monitored by HIPAA COW and success heralded through it.

**Facilitating procurement**

Working with the Wisconsin Department of Administration, DHFS could establish procurement authority for state, county and municipal agencies in the form of a purchasing bulletin for vendors that meet the SMG certification.[v] While private organizations could not buy off the state bulletin, it would expose vendor offerings and pricing. The state bulletin would be a boost to vendors that have obtained certification and would support the national effort by adding another participating state.

Written by Ted Ohlswager, Wisconsin Department of Health and Family Services HIPAA Coordinator

---

[i] Session encryption uses either Secure Socket Layers (SSL) or Transport Layer Security (TLS), both of which use a server level digital certificate.

[ii] "Management Update: Tips on How to Implement Secure Messaging"; October 8, 2003.

[iii] "Secure E-Mail Creates New Model and Minimum Requirement for EBPP"; July 3, 2002.

[iv] Brute Squad Labs, BT Global Services, Syntegra, MailQube, Mitre Corp, Nexor, Novell, PostX, Sigaba, Tovaris, and Tumbleweed.

[v] State statutes (s.16.73(4)(a) and s.16.75(6)) also allow purchases through cooperation with other states and regional nonprofit consortia.